

-63-

**What is claimed is:**

1        1.    A method of processing and storing data in a  
2        computer system including processor circuitry, and a data  
3        storage device, the method comprising the steps of:

4                storing first and second sets of records in  
5        separate first-in, first-out data structures,  
6        respectively, on the data storage device, the first and  
7        second sets of records being of different data  
8        resolutions and corresponding to overlapping periods of  
9        time;

10               operating the processor circuitry to receive  
11        data collected over a period of time; and

12               operating the processor circuitry to update at  
13        least one record in each of the stored first and second  
14        sets of records with the received data such that a  
15        previous record included in each of the first and second  
16        data structures is replaced;

17               periodically collecting network traffic data,  
18        wherein the collected network traffic data includes byte  
19        and packet count information associated with each of a  
20        plurality of monitored conversations between devices  
21        included in the computer system;

22               storing the collected network traffic data in a  
23        buffer; and

24               operating the processor circuitry to retrieve  
25        network traffic data from the buffer, the retrieved  
26        network traffic data being received by the processor  
27        circuitry;

C

-64-

28            wherein the step of operating the processor  
29        circuitry to update at least one record in each of the  
30        stored first and second sets of records includes the  
31        steps of:

32            updating a record corresponding to a first  
33        conversation in the first set of records; and

34            updating a record corresponding to the first  
35        conversation in the second set of records.

1        30. The method of claim 7, further comprising the step  
2        of:

3            allocating fixed amounts of storage space on  
4        the data storage device for storing each one of the first  
5        and second first-in, first-out data structures used to  
6        store the first and second sets of records.

1        31. The method of claim 7, wherein the first set of  
2        records include hourly records and the second set of  
3        records includes daily records.

1        32. The method of claim 7,  
2            wherein the network traffic data stored in the  
3        buffer includes time stamp information indicating the  
4        period of time in which the network traffic data was  
5        collected; and

6            wherein the step of operating the processor  
7        circuitry to update at least one record in each of the

C

-65-

8 stored first and second sets of records includes the step  
9 of:

10 examining at least one time stamp included in  
11 the buffered network traffic data.

1 33. The method of claim 7,

2 wherein the processor circuitry includes first  
3 and second central processing units, and

4 wherein the step of operating the processor  
5 circuitry to update at least one record in each of the  
6 stored first and second sets of records includes the step  
7 of operating the first processor to update the first set  
8 of records while operating the second processor to update  
9 the second set of records.

1 34. The method of claim 7, wherein the computer system  
2 further includes a display device, the method further  
3 comprising the step of:

4 displaying data corresponding to overlapping  
5 periods of time at different resolutions on the display  
6 device.

1 35. A computer system for monitoring network traffic  
2 data comprising:

3 a memory;  
4 a data storage device; and  
5 a processor to execute instructions stored in  
6 the memory,  
7 wherein the memory stores:

-65-

C

-66-

8                   instructions to store first and second  
9   sets of records in separate first-in, first-out data  
10  structures, respectively, on the data storage device, the  
11  first and second sets of records being of different data  
12  resolutions and corresponding to overlapping periods of  
13  time;

14                   instructions to receive data collected  
15  over a period of time;

16                   instructions to update at least one record  
17  in each of the stored first and second sets of records  
18  with the received data such that a previous record  
19  included in each of the first and second data structures  
20  is replaced;

21                   instructions to periodically collect  
22  network traffic data, wherein the collected network  
23  traffic data includes byte and packet count information  
24  associated with each of a plurality of monitored  
25  conversations between devices included in the computer  
26  system;

27                   instructions to store the collected  
28  network traffic data in a buffer; and

29                   instructions to retrieve network traffic  
30  data from the buffer, the retrieved network traffic data  
31  being received by the processor;

-66-  


-67-

32            wherein the instructions to update at least one  
33        record in each of the stored first and second sets of  
34        records include instructions to:

35            update a record corresponding to a first  
36        conversation in the first set of records; and

37            update a record corresponding to the first  
38        conversation in the second set of records.

1        36. The computer system of claim 35, wherein the memory  
2        further comprises instructions to:

3            allocate fixed amounts of storage space on the  
4        data storage device for storing each one of the first and  
5        second first-in, first-out data structures used to store  
6        the first and second sets of records.

1        37. The computer system of claim 35, wherein the first  
2        set of records include hourly records and the second set  
3        of records includes daily records.

1        38. The computer system of claim 35,  
2            wherein the network traffic data stored in the  
3        buffer includes time stamp information indicating the  
4        period of time in which the network traffic data was  
5        collected; and

6            wherein the instructions to update at least one  
7        record in each of the stored first and second sets of  
8        records include instructions to:

-67-  
C

-68-

1           examine at least one time stamp included in the  
2       buffered network traffic data.

3       39. The computer system of claim 35,  
4           wherein the processor includes first and second  
5       central processing units, and  
6           wherein the instructions to operate the  
7       processor to update at least one record in each of the  
8       stored first and second sets of records includes  
9       instructions to operate the first processor to update the  
10      first set of records while operating the second processor  
11      to update the second set of records.

1       40. The computer system of claim 35 further including a  
2       display device, the memory further comprising  
3       instructions to:  
4           display data corresponding to overlapping  
5       periods of time at different resolutions on the display  
6       device.

1       41. A computer program product system for monitoring  
2       network traffic data, said computer program product  
3       comprising a computer usable medium having computer  
4       readable program code means embodied in said medium for  
5       causing a processor in a computer to:  
6           store first and second sets of records in separate  
7       first-in, first-out data structures, respectively, on a  
8       data storage device, the first and second sets of records  
9       being of different data resolutions and corresponding to  
10      overlapping periods of time;

-68-

-69-

1           receive data collected over a period of time;  
2           update at least one record in each of the stored  
3       first and second sets of records with the received data  
4       such that a previous record included in each of the first  
5       and second data structures is replaced;

6           periodically collect network traffic data, wherein  
7       the collected network traffic data includes byte and  
8       packet count information associated with each of a  
9       plurality of monitored conversations between devices  
10       included in the computer system;

11           store the collected network traffic data in a  
12       buffer; and

13           retrieve network traffic data from the buffer, the  
14       retrieved network traffic data being received by the  
15       processor;

16           wherein the causing the processor to update at least  
17       one record in each of the stored first and second sets of  
18       records includes:

19                updating a record corresponding to a first  
20       conversation in the first set of records; and

21                updating a record corresponding to the first  
22       conversation in the second set of records.

-69-

C

-70-

1 42. The computer program product of claim 41, wherein  
2 the computer readable program code means further causes  
3 the processor to:

4 allocate fixed amounts of storage space on the  
5 data storage device for storing each one of the first and  
6 second first-in, first-out data structures used to store  
7 the first and second sets of records.

1 43. The computer program product of claim 41, wherein  
2 the first set of records include hourly records and the  
3 second set of records includes daily records.

1 44. The computer program product of claim 41,  
2 wherein the network traffic data stored in the  
3 buffer includes time stamp information indicating the  
4 period of time in which the network traffic data was  
5 collected; and  
6 wherein the computer readable program code  
7 means to update at least one record in each of the stored  
8 first and second sets of records includes computer  
9 readable program code means to examine at least one time  
10 stamp included in the buffered network traffic data.

1 45. The computer program product of claim 41,  
2 wherein the processor includes first and second  
3 central processing units, and

4 wherein the computer readable program code  
5 means to update at least one record in each of the stored  
6 first and second sets of records includes computer  
7 readable program code means to operate the first

-70-

C



-71-

8 processor to update the first set of records while  
9 operating the second processor to update the second set  
10 of records.

1 46. The computer program product of claim 41 wherein the  
2 computer readable program code means further causes the  
3 computer to display data corresponding to overlapping  
4 periods of time at different resolutions on a display  
5 device.